Region Örebro län

Rapport
Datum: 2023-03-24
Författare: Anneli Björkholm

Årsrapport informationssäkerhet 2022

Version 1

Version: 1

Årsrapport informationssäkerhet 2022

Version 1

Anneli Björkholm och Sofia Öhrman

2023-03-24

Innehåll

1. Sammanfattning

Informationssäkerhet handlar om att skydda information på ett säkert sätt. Det gäller all slags information oavsett var den finns lagrad, exempelvis på papper, digitalt eller muntligt. Information är en av Region Örebro läns (nedan regionen) viktigaste tillgångar. Det är även en förutsättning för en säker och effektiv verksamhet samt en förutsättning för en säker och bra digitalisering.

Regionen ska bedriva ett systematiskt informationssäkerhetsarbete. Det systematiska arbetet med informationssäkerhet och utveckling av regionens säkerhetskultur blir allt viktigare då alltmer information finns tillgänglig digitalt och hanteras/behandlas av olika leverantörer. Detta medför också risker, genom it-attacker kan information göras otillgänglig eller gå förlorad. Riskerna måste därför fångas upp och hanteras, rätt säkerhetskrav måste ställas på leverantörer i rätt tid.

Samhället står inför nya utmaningar i takt med att vår omvärld ständigt förändras. Efter att kriget i Ukraina började under våren 2022 har det världspolitiska säkerhetsläget snabbt förändrats. En del av kriget, som pågår genom riktade it-attacker, s k cyberkrigsföring, inom Europa har medfört att även hotläget har ökat inom hela Europa. Det pågående cyberkriget som sker resulterar i en ökad mängd cyberattacker för att skada myndigheter samt andra offentliga verksamheter, där vissa aktörer inriktar sig specifikt på hälso- och sjukvård.

I detta nya läge blir informationssäkerhetsarbetet inklusive säkerhetskulturen ännu viktigare samtidigt som ny lagstiftning kommer att ställa ännu högra krav på det systematiska informationssäkerhetsarbetet.

Informationsklassningar och riskanalyser behöver ske i verksamheter som hanterar information. Det är grunden i det systematiska informationssäkerhetsarbetet och dataskyddsarbetet som ska finnas i alla regioner och kommuner. Således är det här ett ständigt återkommande arbete för regionen liksom för alla andra organisationer som hanterar information.

De uppföljningar som skett av informationssäkerhetsarbetet och säkerhetskultur i regionen visar på ett fortsatt behov av att öka kunskapen kring informationssäkerhet i stort, i synnerhet kunskapen om ansvar och roller, vem som är informationsägare och vad innebär det att vara informationsägare etc. Områdena uppföljning och utvärdering, upphandling och utveckling av säkerhetskultur är viktiga områden som fortsatt behöver utvecklas.

Uppföljningarna visar vidare att informationsklassningar och riskanalyser till viss del genomförs i organisationen. För att förbättra arbetet i regionen behöver kunskapen stärkas. Vidare finns det ett kvarstående behov av att förbättra verktyget för informationsklassning och riskanalys.

2. Bakgrund

Information är en av regionens viktigaste tillgångar. Det är även en förutsättning för en säker och effektiv verksamhet samt för digitaliseringen. Informationssäkerhet handlar om att skydda information på ett säkert sätt. Det gäller all slags information oavsett var den finns lagrad, exempelvis på papper, digitalt eller muntligt.

Regionen ska utöva ett systematiskt informationssäkerhetsarbete med stöd av den svenska och internationella standarden ISO 27000 för informationssäkerhet och cybersäkerhet samt dataskydd.

Ledningssystem för informationssäkerhet (LIS) ska i tillämpliga delar baseras på SS-ISO/IEC 27001:2017 eller motsvarande likvärdiga principer för ledning och styrning av informationssäkerhetsarbetet, innefattande att samtliga säkerhetskritiska administrativa och tekniska processer ska vila på en formell grund, där roller, ansvar och befogenheter finns tydligt definierade.

I det systematiska informationssäkerhetsarbetet ska hot, sårbarheter och risker identifieras samt säkerhetsåtgärder införas som reducerar dessa till en för regionen acceptabel nivå med hänsyn till konfidentialitet, riktighet och tillgänglighet. Medborgarna ska kunna lita på den information regionen hanterar och att den skyddas på ett bra vis.

Ett systematiskt informationssäkerhetsarbete innebär att strukturerat planera, avsätta resurser, fatta medvetna beslut för att skydda rätt information på rätt sätt. Det systematiska informationssäkerhetsarbete ska bedrivas för att stärka förmågan att undvika negativa händelser som påverkar regionens verksamheter. Inträffar en negativ händelse ska denna kunna hanteras på en godtagbar nivå med bibehållet förtroende från regionens intressenter.

Bedrivs inte informationssäkerhetsarbetet enligt de lagkrav som ställs kan det innebära konsekvenser som att informationssäkerhetsarbetet inte kan bedrivas med den kvalitet som förväntas vilket kan resultera i att regionens informationstillgångar inte hanteras på ett korrekt sätt. Detta kan vidare leda till sanktionsavgifter.

Ledningens genomgång är en viktig del enligt standarden för informationssäkerhet (SS-ISO/IEC 270001:2017) och ett krav enligt Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter inom hälso- och sjukvården (HSLF-FS 2016:40). Syftet med genomgången är att tillsammans med ledningen gå igenom och se över det systematiska informationssäkerhetsarbetet och dess styrning. Årsrapporten för informationssäkerhet är en del av denna genomgång för att säkerställa informationssäkerhetsarbetet och styrningens fortsatta lämplighet, tillräcklighet och verkan.

Denna rapport är framtagen på enheten för juridik och informationssäkerhet. Informationssäkerhetssamordnaren har samlat in material genom enkätuppföljningar och förfrågningar/intervjuer med representanter från alla regionens förvaltningar. Utifrån detta har rapporten sammanställts av informationssäkerhetsamordnaren och enhetschef för juridik och informationssäkerhet. Avsnitt 7.1.1 och 7.1.2 har skrivits av medarbetare på Regionservice IT.

2.1 Informationssäkerhetspolicy

Regionen ska utöva ett systematiskt informationssäkerhetsarbete med stöd av den svenska och internationella standarden ISO 27000 för informationssäkerhet och cybersäkerhet samt dataskydd. Ledningssystem för informationssäkerhet (LIS) ska i tillämpliga delar baseras på SS-ISO/IEC 27001:2017 eller motsvarande likvärdiga principer för ledning och styrning av informationssäkerhetsarbetet, innefattande att samtliga säkerhetskritiska administrativa och tekniska processer ska vila på en formell grund, där roller, ansvar och befogenheter finns tydligt definierade.

Enligt Socialstyrelsens föreskrifter HSLF-FS 2016:40 ska varje vårdgivares ledningssystem innehålla en informationssäkerhetspolicy. I informationssäkerhetspolicyn beskrivs regionens mål och principer för informationssäkerhet för alla verksamheter. Policyn ska bidra till ett professionellt förhållningssätt där informationssäkerhetsaspekter ska vägas in i beslut som rör hantering av information. Policyn omfattar all information oavsett i vilken form den lagras eller hanteras. Nuvarande informationssäkerhetspolicy fastställdes 2015 har uppdaterats en gång tidigare samt senast under 2022. Syftet med uppdateringen var att förtydliga roller och ansvar samt förbättra informationssäkerhetsarbetet.

3. Informationssäkerhetsarbetet i regionen

3.1 Bemanning och organisation

Informationssäkerhetsarbetet i regionen utgår från Enheten för juridik och informationssäkerhet. Där är även informationssäkerhetssamordnaren samt dataskyddsombudet placerade.

Informationssäkerhetssamordnaren arbetar strategiskt med informationssäkerhet. Detta genom att exempelvis säkerställa att styrande och stödjande dokument finns på plats, genomföra utbildningar och informationsinsatser, ge råd och stöd. Arbetet är även av operativ karaktär. Dataskyddsombudets roll är till stor del reglerad genom EU:s dataskyddsförordning, GDPR. Exempelvis ska dataskyddsombudet ge råd och stöd, erbjuda utbildningar men även genomföra tillsyn samt anmäla brister i verksamheterna till Integritetsskyddsmyndigheten, IMY. Enhetschefen för juridik och informationssäkerhet arbetar till övervägande del med informationssäkerhet- och dataskyddsfrågor tillsammans med informationssäkerhetssamordnaren och dataskyddsombudet.

Regionen har ett informationssäkerhetsråd med representanter från samtliga förvaltningar. Informationssäkerhetsrådets uppdrag är att stödja och utveckla regionens systematiska informationssäkerhetsarbete på en övergripande nivå. Rådet och rådets medlemmar utgör en kanal för informationssäkerhetsfrågor mellan regionkansliet och övriga förvaltningar inom regionen. Rådet rapporterar till regionens ledningsgrupp. Informationssäkerhetsrådet har fyra planerade möten per år. Vid behov kan fler möten hållas. Rådet är vidare en remissinstans för ex. styrande dokument.

Rådet besår av följande medlemmar: enhetschef för juridik och informationssäkerhet (ordförande), informationssäkerhetssamordnare, dataskyddsombud, chef säkerhets- och beredskapsenheten, representant för staben för digitalisering, it-säkerhetsansvarig, it- chef, representant från upphandling samt Medicinsk Teknik, förvaltningsövergripande chefläkare, beredskapsläkare samt en representant från övriga regionens förvaltningar.

3.2 Informationssäkerhetsarbetet under 2022

Regionens informationssäkerhetsarbete ska bedrivas systematiskt och riskbaserat. För att hitta rätt nivå av skydd för den information som regionen hanterar är det viktigt att utgå från värdet av informationen och de risker som finns. Det ska göras genom informationsklassning och riskanalys av regionens informationstillgångar. Att regelbundet följa upp informationsklassningar och riskanalyser är av största vikt då regionen måste anpassa sig till en ständigt förändrad och allt mer komplex hotbild.

All information ska ha en identifierad ägare. Informationsägare är den som äger och ansvarar för den information som skapas och används inom verksamheten. Ansvar som informationsägare följer det delegerade verksamhetsansvaret. I de fall där det finns ett flertal informationsägare likställs rollen objektägare med informationsägare enligt regionens förvaltningsmodell för it- stöd.

Under 2022 har it- attackerna fortsatt att öka mot myndigheter och företag både i Sverige och i andra länder. MSB tillhandahåller en sida med löpande information och omvärldsbevakning inom it- säkerhetsområdet som regionen tar del av.

Det finns ett behov av att öka kunskapen kring informationssäkerhet i stort, i synnerhet kunskapen om ansvar, vem som är informationsägare och vad innebär det att vara informationsägare. Informationsklassningar och riskanalyser genomförs till viss del i organisationen med varierande kvalité. Det finns fortsatt ett stort behov av att öka kunskapen i verksamheterna om hur informationsklassningar och riskanalyser sker. Fler personer i verksamheterna behöver utbildas för att kunna genomföra både klassningar och riskanalyser av regionens informationstillgångar.

Under 2022 har enheten för juridik och informationssäkerhet erbjudit flera informationstillfällen och utbildningsinsatser för olika grupperingar i syfte att öka kunskapen. Vidare har styrande och stödjande dokument uppdaterats och tillkommit för att höja kunskapen. Det är dock av stor vikt att fortsätta öka medvetenheten och höja kunskapsnivån generellt. Digitaliseringen går fortsatt väldigt snabbt och här måste informationssäkerheten fångas in i ett tidigt skede.

3.3 Dataskydd

Dataskydd utgör en del av informationssäkerheten. Det är exempelvis genom klassningar och riskanalyser kravställning på dataskydd och säkerhetsåtgärder kan ske. Informationssäkerhet och dataskydd hänger således nära ihop.

Arbetet med att säkerställa att regionens personuppgifter hanteras utifrån GDPR är ett ständigt pågående arbete. För att säkerställa att riktlinjer och rutiner följs kan interna kontroller, utifrån en tillsynsplan, ske årligen av regionens dataskyddsombud. Även oplanerade granskningar kan komma att ske, utifrån händelser i omvärlden eller inom regionen.

3.3.1 Överföring av personuppgifter till tredjeland

En stor del av dataskyddsarbetet handlar om överföring av personuppgifter till tredjeland (dvs. länder utan för EU/EES). Detta mot bakgrund av den s k Schrems II domen som meddelades i juni 2020 av EU domstolen. I domen underkände EU

domstolen överföringsmekanismen Privacy Shield. Privacy Shield kunde tidigare användas som lagligt stöd för att överföra uppgifter till USA. I och med att denna överföringsmekanism underkändes så har möjligheten att överföra personuppgifter till USA starkt begränsats vilket skapat stora utmaningar för regionen liksom andra personuppgiftsansvariga i Sverige och Europa.

Schrems II domen har sedan den kom 2020 gett upphov till ett mycket omfattande och komplicerat arbete med PUB-avtal där leverantörer och underleverantörer har kopplingar till tredjeland, främst USA.

Genom Sjukvårdsregion Mellansveriges informationssäkerhetsgrupp påbörjades under 2022 ett samarbete med att ta fram en gemensam vägledning för hantering av överföringar av personuppgifter till tredjeland Under 2022 färdigställdes vägledningen och denna kan verksamheterna använda vid bedömning om lagligheten av behandling av personuppgifter i tredjeland en samt som stöd vid avtalsskrivandet.

Under 2022 har en ny riktlinje inklusive mall om konsekvensbedömning enligt GDPR tagits fram. I vissa fall ska en konsekvensbedömning ske enligt GDPR, dvs. gällande personuppgiftsbehandlingen. Det är av stor vikt att nu få igång arbetet med just konsekvensbedömningarna i regionen.

3.3.2 Microsoft Office 365 och Teams

Under våren 2021 beslutades att regionen skulle införa en hybridintegration med Microsoft 365. En hybridlösning innebär att verksamheterna avgör vilken information som ska lagras lokalt och vad som ska lagras i molnet. Inför detta beslut gjordes en rättsutredning om Microsoft Office och Teams.

Teams har införts stegvis i två faser under 2021/2022 där fas ett innebär tillgång till chatt och mötesbokningar samt möten i Teams. Fas två innebär tillgång till att skapa team för grupper eller projekt, samarbeta, dela filer och använda verktyg som Planner, Forms och OneNote.

Informationssäkerhetssamordnare och jurist har varit delaktiga i arbetet med informationsklassning och riskanalys för införande av Teams som har letts av extern konsult.

Efter genomförd klassning och riskanalys påbörjades och slutfördes under 2022 ett arbete med att ta fram riktlinje, utbildningsmaterial och annan stödjande information i syfte att tydliggöra hur och när Teams kan användas och vilken information som får hanteras i Teams.

Under hösten 2022 påbörjades också ett arbete med att genomföra en konsekvensbedömning enligt GDPR av Teams och den personuppgiftsbehandling som sker däri. Resultatet av konsekvensbedömningen ska sedan presenteras för objektägaren (dvs. informationsägaren).

3.4 Externa och interna samarbeten

3.4.1 Informationssäkerhetsgruppen i Sjukvårdsregion Mellansverige

I takt med digitaliseringen har samarbetet mellan regionerna stärks, främst inom Sjukvårdsregionen Mellansverige och genom informationssäkerhetsgruppen.

Informationssäkerhetsgruppen är underställd samverkansnämndens ledningsgrupp. Informationssäkerhetsgruppen består av medlemmar från sjukvårdsregionens sju regioner. Gruppens huvuduppgift är att utveckla samarbetet inom informationssäkerhetsområdet inklusive dataskydd och cyberssäkerhet, öka kompetensen inom området och synliggöra det samarbete som sker.

I arbetsgruppen ingår regionernas informationssäkerhetssamordnare/chefer, dataskyddsombud, jurister samt resurser med it-säkerhetskompetens. Under 2022 har fyra digitala möten genomförts.

3.4.2 Hälso- och sjukvårdens informationssäkerhetsnätverk, HoSiS

HoSiS är främst ett nätverk för de som arbetar med eller har ett ansvar för arbetet med informationssäkerhet inom regionernas hälso- och sjukvård i Sverige.
Syftet med nätverket är att ge de personer som har ett uppdrag att samordna och stödja arbetet med hälso- och sjukvårdens informationssäkerhet i regionerna möjlighet att utbyta kunskap och information med varandra.

Målet är att genom att delta i nätverksträffar erbjuda medlemmar ett stöd för sitt arbete inom informationssäkerhetsområdet i den egna organisationen samt att tillhandahålla ett forum för utbyte och omvärldsbevakning. Ambitionsnivån med nätverket är att stödja och styra aktiviteter utifrån gemensamt framtagna fokusområden samt att informera om SKR:s och MSB:s kommande aktiviteter.

3.4.3 Informationssäkerhetsnätverk i Örebro län

I länet finns ett nätverket bestående av deltagare från transportstyrelsen, Örebro kommun, SCB, Försvaret, Örebro Universitet, länsstyrelsen och regionen. Deltagarna arbetar med informationssäkerhet och/eller it- säkerhet.

Nätverket har träffats två gånger under 2022. Fokus för nätverket är informationssäkerhetsfrågor kopplat till de attacker som har ökat i vårt samhälle och

hur de olika myndigheterna arbetar med dessa. En direkt kanal har skapats mellan deltagande verksamheter för att snabbt dela information om pågående hot.

3.4.4 Regionservice IT-SIRT

År 2020 startades IT-SIRT (IT security Incident response Team). Syftet är att teamet ska hålla sig välinformerad om aktuella hot och inträffade säkerhetsincidenter inom regionen samt i omvärlden samt för att säkerställa att olika hotbildscenarier och säkerhetsincidenter kan hanteras och proaktivt verka för ökad säkerhet. Informationssäkerhetssamordnare deltar i IT- SIRT gruppens regelbundna avstämningar.

3.4.5 Regionövergripande kunskapsutbyte inom it- och cybersäkerhet

Gruppen startades 2022 i samband med log4j incidenten som drabbade alla regioner. I gruppen ingår representanter från Sveriges regioner och träffas 4-5 ggr/år. Syftet med gruppen, där alla regioner ingår, är att dela kompetens och erfarenheter gällande verktyg och arbetssätt m.m. inom it- och cybersäkerhetsområdet.

3.4.6 Övriga samarbeten

Förutom ovan nämnda samarbeten sker regelbunden avstämning mellan informationssäkerhetssamordnare och it- säkerhetsansvarig för informationsutbyte och diskussion avseende aktuella frågeställningar inom informationssäkerhetsområdet.

4. Granskningar och skyddsåtgärder

4.1 Informationsklassning och riskanalys

Risker som påverkar regionens informationssäkerhet ska identifieras, analyseras och behandlas samt återföljas av kontinuerlig uppföljning. Beslut om olika lösningar ska baseras på bedömd risk och informationstillgångarnas klassificeringsvärde. Informationsklassning är grunden för att genomföra en riskanalys då riskanalysen baseras på informationens värde.

Informationsägare är den som äger och ansvarar för den information som skapas och används inom verksamheten. Ansvar som informationsägare följer det delegerade verksamhetsansvaret.

Det finns ett fortsatt ett behov av att öka kunskapen i verksamheterna när det gäller det systematiska informationssäkerhetsarbetet. Fler personer i verksamheterna behöver kunna genomföra riskanalyser och informationsklassningar av regionens informationstillgångar. Informationsklassningar och riskanalyser är grunden i det

systematiska informationssäkerhetsarbetet. Detta är således något som måste bli en naturlig del av all informationshantering, exempelvis vid upphandlingar, inköp, drift och förvaltning av it- stöd samt för hantering av information i verksamheternas processer.

4.2 Granskningar

Ingen extern granskning eller tillsyn har utförts eller ägt rum under 2022.

4.3 Skyddsåtgärder

4.3.1 Loggning och logguppföljning

Loggning och logguppföljning är en viktig del i regionens arbete med patientsäkerhet. Framför allt för att kunna visa att regionens hantering av personuppgifter sker på ett legalt och riktigt sätt men också för att kunna utreda misstankar om otillåten hantering av personuppgifter. Regionen är enligt lag skyldig att föra logg över elektronisk åtkomst inom vårdgivarens verksamhet och dokumentera regelbunden och systematisk loggkontroll.

Loggsystemet var tidigare ett s k oförvaltat system men under 2022 kom loggsystemet in i den ordinarie systemförvaltningen och tillhör nu Vårdsystem. Under 2021 och 2022 har även ett arbete påbörjats med att strukturera om arbetet med logghanteringen bland annat mot bakgrund av att systemet blivit ett förvaltat system.

Under 2022 har 231 patienter begärt ut loggar över vilka anställda som tagit del av deras journaluppgifter. Därutöver uppkommer olika situationer som gör att verksamhetschefer efterfrågar loggar på medarbetare, det kan t.ex. vara kompletterande uppgifter till de slumpvisa loggarna eller att verksamhetschefen fått till sig uppgifter som rör misstanke om otillåten/obehörig åtkomst som måste granskas och kontrolleras vidare.

5. Uppföljningar

5.1 Uppföljning av informationssäkerhetsarbetet i regionen Intern styrning och kontroll (ISK)

Intern styrning och kontroll (ISK) är en process där regionstyrelsen, nämnderna och verksamhetsledningar har för att tillsammans upprätthålla en effektiv ledning och styrning av verksamheten. Processen ska säkerställa en ändamålsenlig och lagenlig verksamhet, det vill säga att verksamheten bedrivs i enlighet med de krav som ställs på verksamheten. För att säkerställa att kraven är uppfyllda finns i uppföljningen av ISK-processen beskrivningar av risken samt vad som förväntas av förvaltningarna när

det gäller rapportering av informationssäkerhetsarbetet. När det gäller informationssäkerhetskraven ska dessa vara tillgodosedda utifrån kraven på konfidentialitet, riktighet, tillgänglighet samt spårbarhet.

För att säkerställa att kraven var uppfyllda under 2022 fanns i uppföljningen av ISK-processen beskrivningar av risken samt vad som förväntades av förvaltningarna när det gäller rapportering av informationssäkerhetsarbetet.

Risken att verksamheten inte efterlever tillämplig dataskyddslagstiftning (GDPR och patientdatalagen) samt NIS-direktivet som implementerats genom lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Regionövergripande åtgärder inför 2022:

- Säkerställa ett systematiskt och riskbaserat informationssäkerhetsarbete med användande av de resurser som i prioritering i förhållande till andra angelägna verksamheter, kan anslås.
- All berörd personal ska ha god kunskap om och medverka till att följa regelverk för informationssäkerhet.
- Att informationsklassa och riskbedöma vid inköp, upphandling och förändring som kan påverka informationssäkerheten.

Förvaltningarna har rapporterat för 2022. I rapporteringen framgår att informationsklassning och riskanalys genomförs särskilt vid upphandling av it- stöd. Vissa förvaltningar har avsatt resurser för sitt informationssäkerhetsarbete. För att öka kunskapen om roller och ansvar samt förståelsen för vad ett systematiskt informationssäkerhetsarbete är behövs informationsinsatser då ett systematiskt riskbaserat informationssäkerhetsarbete kräver kontinuerlig översyn och uppföljning för att motverka eventuellt nya uppkomna säkerhetsbrister.

5.2 Enkätuppföljning – i syfte att mäta kunskap och informationssäkerhetskultur i regionen

Ett regeringsuppdrag ställdes till MSB (Myndigheten för samhällsskydd och beredskap) 2021 för att mäta framförallt förutsättningen för det systematiska informationssäkerhetsarbetet och i vilken utsträckning som det systematiska arbetet bedrivs i regioner och kommuner. De angivna svaren genererades in enligt en uppföljningsmodell som delade in det systematiska informationssäkerhetsabetet i fyra nivåer:

- Nivå 1: organisationer som har grunderna i informationssäkerhetsarbetet
- Nivå 2: organisationer som bedriver informationssäkerhetsarbetet med viss systematik och är bättre på grunderna
- Nivå 3: organisationer som har ett kvalificerat innehåll i informationssäkerhetsarbetet samt är bättre på både grunderna och systematiken
- Nivå 4: organisationer som arbetar avancerat med ständiga förbättringar samt är bättre på grunderna, systematiken och innehållet

Resultat 2021

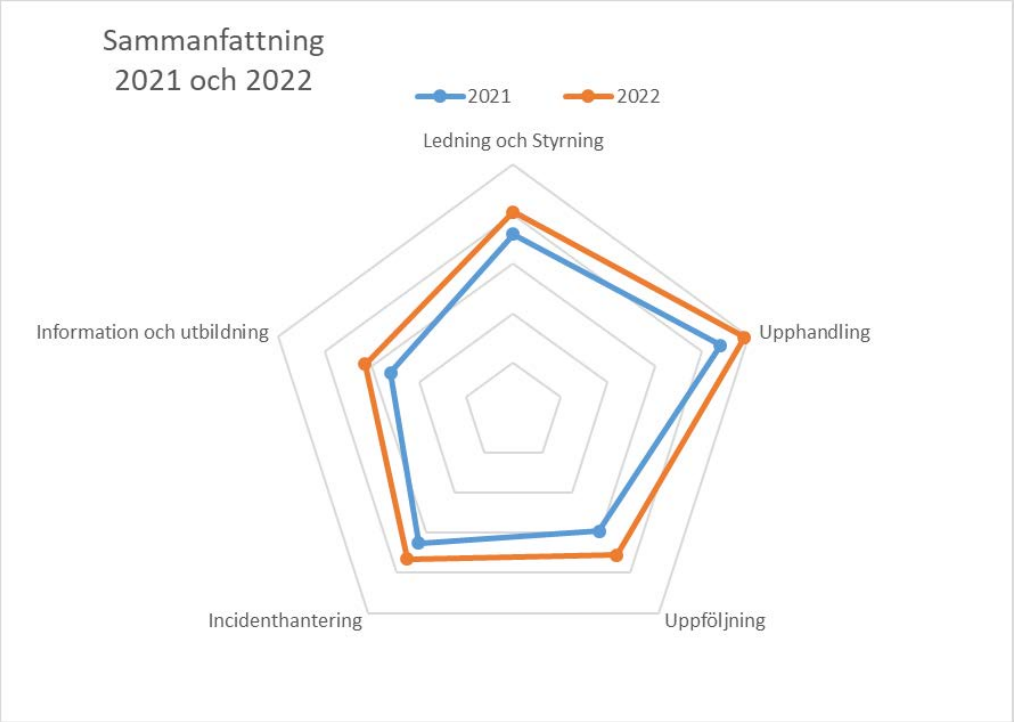
Ett första steg för regionen är att uppnå alla delar i nivå 1. MSB planerar en ny mätning under 2023.

5.2.1 Intern enkät

En enkät riktad primärt till informationsägare i de olika förvaltningarna skickades ut 2021 och en uppföljande enkät 2022 via medlemmarna i informationssäkerhetsrådet. Frågorna i enkäterna handlar om grundläggande kunskaper om innehållet i exempelvis informationssäkerhetspolicy, riktlinjer och rutiner gällande informationssäkerhet. Syftet med enkäterna är att mäta och följa upp resultatet av de genomförda utbildningsinsatserna, och andra insatser under året, samt få en bild av kunskapsnivån och informationssäkerhetskulturen i regionen.

En sammanfattning av resultatet fördelat på mätområden ses nedan:

Den yttre ringen i nedan skala är motsvarande nivå 1 enligt MSB:s modell



Sammanfattade mätområden och innehåll:

Ledning och styrning
Kännedom om policy, riktlinjer och rutiner samt roller och ansvar som är kopplade till informationssäkerhet.

Upphandling
Frågor om informationsklassning och riskanalys i samband med upphandling samt tecknande av personuppgiftsbiträdesavtal med leverantör i de fall som behandling av personuppgifter sker av extern leverantör.

Uppföljning
Frågeställningar för uppföljning av åtgärder av it- incidenter, personuppgiftsincidenter, informationsklassningar samt riskanalyser.

Incidenthantering
Frågeställning kopplade till uppföljning samt medarbetarnas kännedom om vad it-incidenter och personuppgiftsincidenter är.

Information och utbildning
Frågor som är kopplade till ansvar att informera medarbetare om de riktlinjer och rutiner som är framtagna gällande exempelvis användning av digitala mötesverktyg.

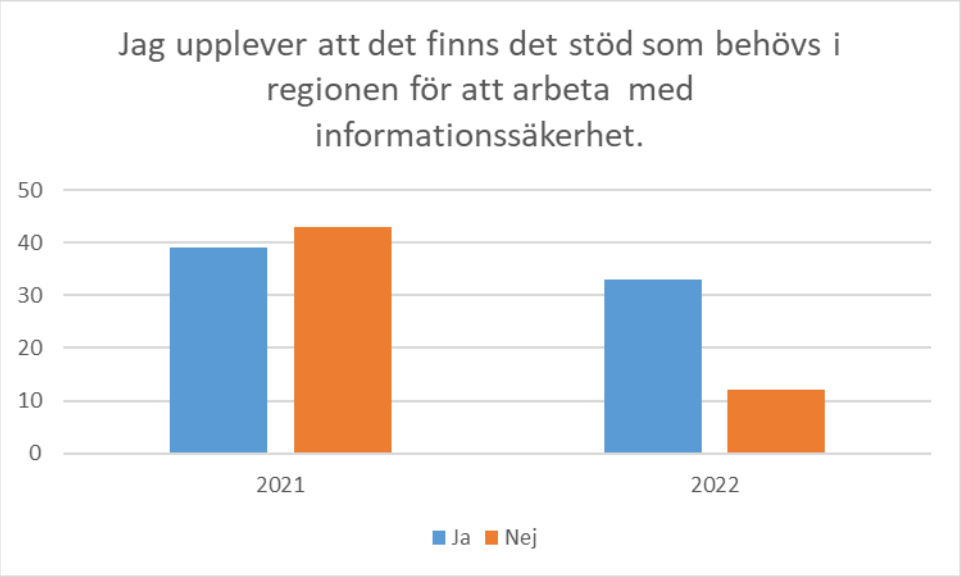
Det sammanställda resultatet visar att regionen är på rätt väg men att mer information och kunskap behövs i de grundläggande delarna som exempelvis roller och ansvar.

Verksamheterna efterlyser stöd i sitt systematiska informationssäkerhetsarbete när det gäller utförande av informationsklassningar och riskanalyser av den klassade informationsmängden samt vid tecknande av PUB-avtal. Det systematiska informationssäkerhetsarbetet genomförs men med hjälp av central eller annan funktion. Enligt enkätsvaren ”genomförs med central eller annan funktion inom verksamheten” är uppfattningen att ansvaret till stor del ligger på Regionservice IT, Medicinsk Teknik samt upphandlingsavdelningen. Det är dock informationsägaren som bär ansvaret för att informationsklassningar och riskanalyser samt uppföljningar sker.

Resultatet av enkäten visar på en ökad kunskap för att det systematiska arbetet ska genomföras, även om det inte utförs av verksamheterna där den ansvarande rollen informationsägare är. I regionen behövs kunskap om informationssäkerhet och vad som ingår i informationssäkerhetsarbetet stärkas, bland annat när det gäller innebörden av roller och ansvar. Men resultatet ser bättre ut nu i jämförelse med MSB:s mätning.

En sammanställning av enkätfrågor och svar finns i bifogad bilaga till rapporten.

5.2.2 Sammanställning av synpunkter från verksamheten om avsaknad av stöd

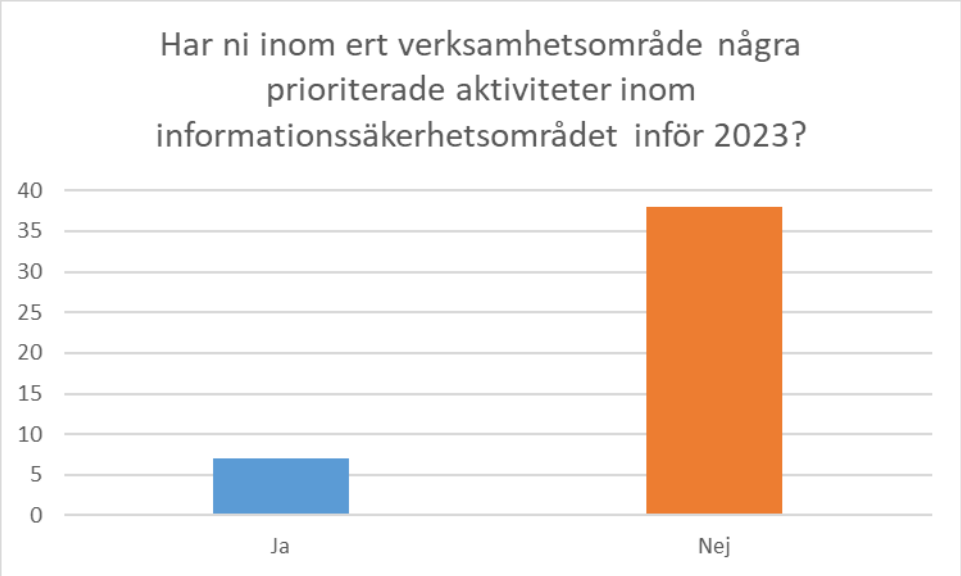


Informationssäkerhetsarbetet har ökat i regionen och stödet i arbetet upplevs som bättre jämfört med 2021. Det finns fortsatt en efterfrågan om stöd och hjälp i form av utsedda funktioner som är lätta att tillgå inom verksamheten för att genomföra de grundläggande delarna i det systematiska informationssäkerhetsarbetet.

Sammanfattning av synpunkter som framkommit från enkätsvar (i fritextfält):

- Svårigheter att finna relevant information- och stödmaterial.
- Behovet av stöd i det praktiska informationssäkerhetsarbetet är stort.
- Alla förvaltningar behöver stöd för dialog och vägvalsfrågor, det stödet saknas idag.
- Få dedikerade resurser för arbetet med informationssäkerhet.
- Ett stort och omfattande område, svårt att ha kontroll på alla delar.
- Osäkerhet gällande GDPR.

5.2.3 Sammanställning av de prioriterade aktiviteter i verksamheterna som rapporterats in via enkäten



Ett fåtal förbättringsåtgärder har angetts i årets enkät, vilket troligen beror på en ansträngd situation gällande resurser.

Planerade aktiviteter för 2023 som har inrapporterats:

- Stödja medarbetare i informationssäkerhetsarbetet genom att delta i grupperingar kopplade till informationssäkerhet i regionen.
- Lyfta behovet av dialoger inom informationssäkerhetsområdet.
- Genomgång av rutiner och vart information finns på intranätet för nya medarbetare.

- Nya medarbetare ska genomgå e- learningsutbildning för informationssäkerhet i PingPong.
- Arbeta aktivt med ansvar och säkerhet vid digitala möten.
- Säkra autentiseringen genom att ″authenticator″ installeras på samtliga datoranvändare.

6. Förbättringsåtgärder

Här nedan följer de förbättringsåtgärder som rapporterats av förvaltningarna för 2022.

6.1 Genomförda planerade aktiviteter 2022

6.1.1 Hälso- och sjukvårdsförvaltningen

En ny tjänst har tillsatts, en informationssäkerhetshandläggare för att operativt stötta verksamheten med informationssäkerhetsfrågor såsom informationsklassning och riskanalyser.

Det har genomförts ett flertal informationsklassningar och riskanalyser i samband med anskaffning, upphandling och vid förändringar som påverkar informationshanteringen. Även uppföljning av befintliga informationsklassningar och riskanalyser har genomförts för befintliga it- lösningar.

6.2 It- lösningar och it- säkerhet

6.2.1 Folktandvården

En upphandling av ett nytt tandvårdssystem är påbörjad.

En lösning för säkra meddelanden har införts. Detta i syfte att på ett säkert sätt dela och ta del av journalinformation mellan privat tandvård och patienter inom folktandvården. Lösningen som är i produktion är en OnPrem lösning (lokal installation på regionens servrar). Ett vidare arbete pågår nu med att säkerställa flöden i verksamheten.

Ett arbete pågår med att gå igenom ett antal it- system som körs via molntjänster och säkerställa att personuppgifter hanteras på korrekt sätt i hela flödet.
Ett arbete har genomförts baserat på informationsklassningar och riskanalyser som grund för ett pågående arbete med avtal med leverantör. En ny beställningsrutin baserad på informationsklassning och riskanalys för det aktuella it- stödet har även skapats för verksamheten.

6.2.2 Folktandvården

Ett införande av multifaktorautentisering (MFA) pågår för alla system i verksamheten. Införande av MFA är också en del i arbetet vid införande av ett nytt tandvårdssystem.

En kontinuitetsplan är framtagen för it- systemen.

6.2.3 Regionservice IT

En uppgradering av infrastruktur versionshantering av databaser har skett.

6.3 Utbildning och information

6.3.1 Folktandvården

En informationsinsats har genomförts inom verksamheten riktad till ledningsgrupp, chefer och medarbetare för att sprida kunskap angående roller och ansvar inom informationssäkerhet. Informationen har anpassats till olika roller och ansvar. En tydlighet har beslutats av ledningsgruppen och delgivits verksamhetschefer av deras ansvar att medarbetare får information och utbildning inom informationssäkerhet. En lathund har tagits fram för att underlätta för verksamhetschefer att hitta information angående it- säkerhet. Information om dataintrång tas upp årligen och extra om det sker avvikelser.

6.3.2 Regionservice, upphandlingsavdelning

Utbildningsinsatser av representanter från Enheten för juridik och informationssäkerhet har genomfört under året. Dessa tillfällen har sedan legat till grund för avdelningsspecifika informations- och diskussionstillfällen med fortbildning och kunskapsöverföring till våra nya medarbetare. Arbetet har också inneburit en ökad förståelse om olika roller och ansvar gällande informationssäkerhetsarbetet Det har resulterat i att upphandlingen kan erbjuda ett bättre stöd åt de verksamheter som upphandlingen arbetar på uppdrag åt. Löpande vid upphandlingar informeras verksamheterna om vad det i en upphandlingssituation innebär att de är informationsägare. Det innefattar såväl det förberedande arbete som ska ske inför en upphandling.

6.3.3 Regionservice, Medicinsk teknik

Inför kommande upphandlingar 2023 informeras verksamheterna om roller och ansvar utifrån ett informationssäkerhetsperspektiv vid upphandling. Det innefattar såväl det förberedande arbete som ska ske inför en upphandling. Medicinsk Teknik stödjer hälso- och sjukvårdsförvaltningen via ett samarbete med hälso- och sjukvårdens informationssäkerhetshandläggare för att införa detta i relevanta rutiner.

6.4 Ett verktyg för informationsklassning och riskanalys

Regionen har idag verktyget ISAK för informationsklassning. Isak är en äldre Excelfil som är framtagen tillsammans med Region Dalarna. Verktyget/Excelfilen innehåller en mall för informationsklassning och riskanalys samt kravställning utifrån de tre säkerhetsaspekterna. ISAK är framtagen för att utföra informationsklassning riktat till it- stöd. För att bedriva ett systematiskt informationssäkerhetsarbete ska all information klassas oavsett var i verksamheten den finns. Det kan exempelvis handla om system, processer eller arbetsflöden där olika informationsmängder hanteras. Detta arbete försvåras idag eftersom ISAK primärt är lämpat för informationsklassning av it- stöd.

SKR har under 2021 och 2022 tagit fram ett webbaserat verktyg för informationsklassning och riskanalys, KLASSA, för att stödja kommuner och regioner i informationssäkerhetsarbetet med möjlighet att genomföra en informationsklassning och riskanalys kopplat till it- stöd, enskilda dokument och processer. Regionens informationssäkerhetssamordnare har varit delaktig arbetet tillsammans med SKR och andra regioner och har därmed haft möjlighet att påverka hur klassningsverktyget på ett lämpligt sätt ska kunna stötta verksamheterna i sitt arbete med informationsklassning och riskanalyser.

KLASSA bygger på modellen för informationsklassning enligt MSB:s metodstöd för systematiskt informationssäkerhetsarbete utifrån standard (SS-ISO/IEC 27001:2017) för ledningssystem och innehåller fyra delar: informationsklassning, kravställning/handlingsplan, upphandlingskrav och riskanalys. KLASSA innehåller vidare utbildningsmaterial och stödjande texter för informationsklassning och riskanalys som tillses av SKR.

Regionens informationssäkerhetssamordnare fortsätter att bevaka och delta i arbetet med KLASSA.

6.5 Utbildningsinsatser

Ett flertal utbildningar genomförs löpande. Exempelvis utbildning för chefer inom ramen för Formellt ledarskap, utbildning för ST-läkare, utbildning för BT-läkare, utbildning för studerande vid läkarprogrammet termin 8 ”Juridik, informations- och patientsäkerhet”.

Informationsinsatser har skett gällande roller och ansvar kopplat till informationssäkerhetsarbetet till ett fåtal/antal ledningsgrupper. Vidare har informationsinsatser om hur informationsklassningar och riskanalyser ska ske ägt rum, även dessa till ett fåtal grupper i regionen.

Det finns en rekommendation att samtliga anställda ska genomföra den e-learningutbildning om informationssäkerhet (DISA) som finns att tillgå i regionens utbildningsportal PingPong. DISA är en utbildning som MSB har tagit fram som tar upp olika aspekter av informationssäkerhet. Utbildningen består av kortare filmer samt påståenden med efterföljande frågor. Utbildningen tar bland annat upp; säkert beteende, lösenord, e-post, skadlig kod, sociala medier, mobila enheter, molntjänster, säkerhetskopiering och loggning och spårbarhet.

7. Incidenter/avvikelser

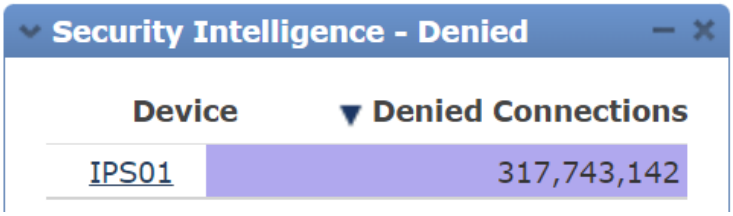
Incidenter och avvikelser sker ofta genom systemfel och misstag. System och infrastrukturen är i dag både stora och komplexa samtidigt som de yttre hoten ökar i takt med digitaliseringen och vår föränderliga omvärld. Ett systematiskt informationssäkerhetsarbete är ett stöd vid kravställning av säkerhet och administrativa rutiner. Verksamheterna behöver därför prioritera informationssäkerhetsarbetet genom att tillsätta tid för kartläggning av processer och identifiering av informationstillgångar, identifiera informationsägare, genomföra informationsklassningar med tillhörande riskanalys och när krav ställs genomföra konsekvensbedömning.

7.1 IT incidenter, ransomware och phising mm

7.1.1 Granskade och stoppade intrång via internet

Regionens intrångsskydd (IPS = Intrusion Prevention System) arbetar utifrån två huvudprinciper, det stoppar trafik utifrån avsändar-/destinationsadress och det analyserar övrig trafik efter ”signaturer” (dvs. kännetecken) som tyder på skadligt beteende. Regionen har ett abonnemang och det kommer fortlöpande information till regionen om svartlistade adresser och intrångs-signaturer som är förknippade med it-brottslighet och skadlig mjukvara.

Den första sortens trafik (från/till svartlistade adresser) var som högst i början på året kring tiden när kriget i Ukraina startade. Nivån låg då på ca en miljon blockerade requests per dag. Nivån ligger i december på ca femhundra tusen blockerade requests per dag. Antal blockerade requests pga. svartlistning under det senaste året:

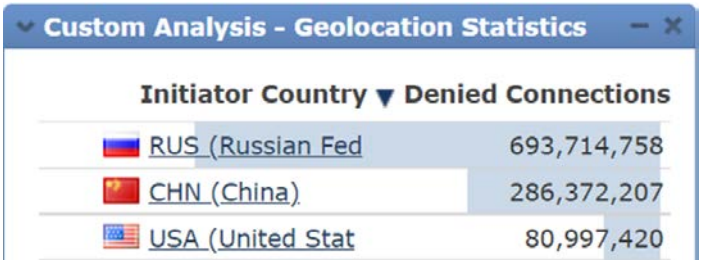


Det mesta av denna trafik genereras säkerligen av automatiska genomsökningar efter sårbarheter, men en del är också manuellt initierade attackförsök. Denna sorts bakgrunds-brus pågår hela tiden, utan avbrott, och blockeras direkt av intrångsskyddet. ”300 miljoner blockeringar” betyder inte att miljontals olika hackers har försökt attackera regionen utan det innebär att ett antal ihärdiga förövare eller automatiserade processer har försökt många tusentals gånger var.

Den andra sortens trafik (som matchar signaturer och kan tyda på mer riktade attacker) har varit mera konstant över tid men den var också hög i början på 2022. I detta fall så var det dock framför allt den s k ”Log4J-sårbarheten” som stod för volymen. Denna mycket allvarliga sårbarhet hanterades, med mycket möda, kring årsskiftet 2021/2022. I stort sett alla företag och organisationer med koppling till internet behövde skyndsamt täppa ingen detta hål i säkerheten. It- brottslingar var inte sena att börja utnyttja sårbarheten och det syntes i statistiken i form av ett ökat antal intrångsförsök.

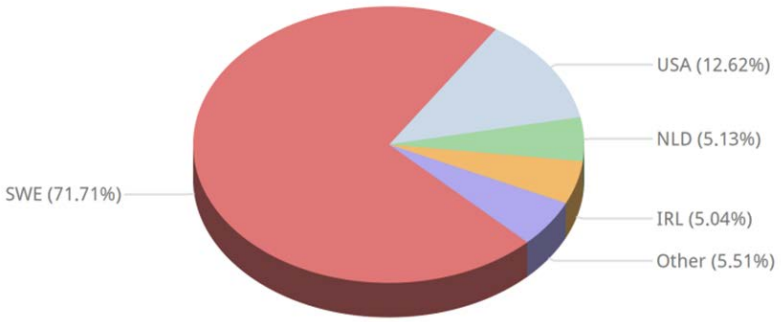
På grund av det ökade hotläget så togs beslut om att ”Geo-blockera” trafik till/från vissa länder. De absolut mest aktiva länderna med offensiva it-aktiviteter har i detta fall varit Ryssland och Kina. Följande siffror visar blockerade requests från Ryssland, Kina och USA. Mängden trafik från Ryssland har varierat över tid men har tidvis varit flera miljoner request per dag.

Antal blockerade requests pga. geoblockering under det senaste året:



Nedanstående diagram visar fördelning av tillåten trafik vid en specifik tidpunkt och representerar inte medel över hela perioden. Regionen har inte möjlighet att få ut denna typ av statistik över en längre period. Det kan noteras att det land regionen kommunicerar mest med är Sverige, USA, Irland och Holland.

Trafik mot regionen, fördelning per sourceland:



7.1.2 E-post filter

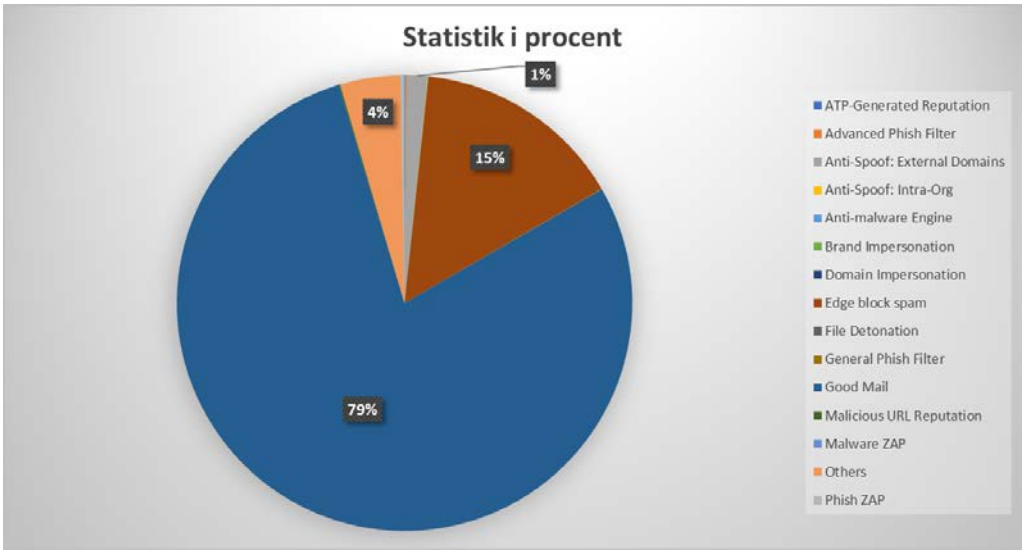
Det e-postfilter som regionen använder är Exchange Online Protection från Microsoft. Det är en extern tjänst utanför regionens datahallar som kontrollerar mailflödet innan mail släpps in i regionens miljö. E-postfiltret har också funktionen att sätta inkommande misstänkta mail i karantän där mottagaren, och administratörer, kan granska mailen utanför regionens egen miljö för att kunna släppa in mail som av mottagaren bedöms vara ok. Baserat på hur mailen i karantän hanteras kommer filtret att ”lära sig” hur inkommande mail bör klassificeras.

Merparten av de blockerade mailen klassar filtret som "Spam" eller "Skräppost".
I de fall ett mail innehåller en av tjänsten ej provad och godkänd länk så skrivs länken om så att man först landar hos den externa tjänsten som undersöker målsajten, vilket minskar risken avsevärt för att klicka på en skadlig länk. Mail från mailservrar på ökända IP-adresser blockeras och listorna på adresser underhålls löpande.

Regionen vitlistar inte e-postadresser. Det rådande säkerhetsläget medger inte det.
En av de vanligaste orsakerna till att mail fastnar i filtret är att det inte går att verifiera att avsändaren är vad eller vem den utger sig för att vara. Det som visas som avsändare är väldigt lätt att förfalska (spoofa) och utnyttjas frekvent i phishingattacker. Noterbart är att om det mailsystem som avsändaren använder inte är rätt konfigurerat så går det inte att spåra vem avsändaren är vilket kan medföra att legitima mail fastnar i karantän p.g.a. spårbarhetsregler.

Totalt under år 2022 har det till alla regionens domäner adresserats nästan 11 miljoner mail. Av totalen har ca 2,3 miljoner mail blockerats, det mesta har klassats som spam sedan kommer blockering p.g.a. förfalskade avsändaradresser (spoofing) högt i statistiken.

Under perioden 2022-02 – 2022-03 var det ett ovanligt högt inflöde av spam men under resten av året följer inflödet av spam samma veckovisa mönster där det egentligen inte sticker ut några värden sett över året. Ur statistiken från mailfiltret går det att se vad som av en eller annan anledning har stoppats och i viss mån varför. Det går inte att se vilket innehåll som har släppts igenom utan någon åtgärd.



7.2 Världsomfattande hotbild

Hela samhället står inför nya utmaningar i takt med att vår omvärld ständigt förändras. Regionen måste anpassa sig till en ständigt förändrad och allt mer komplex hotbild. Svenska verksamheter inom sjukvård utsattes för 869 cyberattacker i veckan under juli - september 2022. Det visar en rapport från Check Point Research. Antalet innebär en tydlig ökning jämfört med motsvarande period 2021.

Även om en cyberattack mot ett sjukhus inte stänger ner ett sjukhus helt så kan den slå ut digital teknik och begränsa tillgången till digital information under en period såsom medicintekniska it- stöd, patientjournaler och vårdrekommendationer. Försvarsmakten utsattes för en it- attack som ledde till att webbplatsen var otillgänglig i 10 minuter. Detta var kort efter att A-kassan var utsatt för en it- attack. It-attacken genererade att A-kassan stängde ner sina system under några veckor. Detta ledde till att 30 000 – 35 000 arbetslösa inte kunde få ut sin ersättning i tid.
I den ökade mängd cyberattacker som i dag pågår i Europa inriktar sig vissa aktörer specifikt på hälso- och sjukvård.

Det systematiska informationssäkerhetsarbetet är därför extra viktigt genom att analysera hotbild och risker. Världen har förändrats och det är av vikt att vara uppmärksam på både attacker och påverkanskampanjer och arbeta så proaktivt som möjligt genom samverkan, omvärldsbevakning samt identifiera tänkbara risker.

7.3 Driftavbrott it- system

I augusti inträffade en incident i regionens passersystem vilket innebar att medarbetare inte kunde komma in till sina arbetsplatser med sina e-tjänstekort. Detta berörde ett flertal områden inom regionen. I samband med detta skickades det ut felaktiga meddelanden till medarbetare med text ” anställningen har upphört”. Passersystemen uppdateras två gånger per dygn för att hålla systemen uppdaterade med eventuella förlorade och spärrade passerkort eller avslutade anställningar. Passersystemen tillses med information från KOLL med anställdas uppgifter om anställning och placering inom regionen. Orsaken till detta var ett fel i den information som KOLL levererade till passersystemen. En lösning är nu framtagen för att felet inte ska uppstå igen.

När det gäller driftavbrott i vårdsystemen har det rapporterats ett antal sådana av mindre karaktär. Dock inte något som avviker från det normala.

7.4 Personuppgiftsincidenter

Under 2022 har det registrerats 118 personuppgiftsincidenter i Platina, av dessa är det 29 incidenter som anmälts vidare till Integritetsskyddsmyndigheten, IMY. Det som är återkommande är kallelse/brev som skickas till fel patient.

8. Fokusområden 2023

8.1 Det systematiska informationssäkerhetsarbetet

Regionen behöver fortsatt förbättra informationssäkerhetskulturen. Kunskapen och medvetenheten behöver öka för de krav som ställs vid behandling av information i alla former. Informationssäkerhetsarbetet kan då bli mer effektivt och systematiskt och ge mera nytta för regionen i helhet.

Genom det systematiska och riskbaserade arbetet ökar kunskapen, avvikelser upptäcks tidigt och kan åtgärdas och allvarliga störningar kan undvikas. All information och de kritiska it- stöden inom regionen ska skyddas och det ska tillses att informationen är riktig och tillgänglig när den behövs. Vidare behöver även säkras att regionens verksamhet kan bedrivas med så liten konsekvens som möjligt om en incident inträffar genom att snabbt kunna reducera och återgå till normalläge.

En viktig del under 2022 var att få ett ledningssystem för informationssäkerhet (LIS) på plats. Ett ledningssystem som är vägledande i de olika faserna i det systematiska informationssäkerhetsarbetet samt innehåller de ”verktyg” som behövs för att bedriva arbetet. De befintliga styrande dokumenten har setts över för att uppdateras och nya har skapats och utgör bas för innehållet i ledningssystemet. Ledningssystemet är nu framtaget och benämns som ”Process för det systematiska informationssäkerhetsarbetet”. Det innehåller mallar för det systematiska arbetet, stöddokument som beskriver hur arbetet ska utföras (Principer och arbetssätt), beskrivning för roller och ansvar, policy och riktlinjer.

Det är en utmaning är att öka kunskapen och bygga upp en kompetens kring informationsklassningar och riskanalyser. I takt med den snabba digitalisering som nu sker märks också att denna kompetens ofta efterfrågas.

Informationsklassningar och riskanalyser kommer alltid att behöva ske i verksamheter som hanterar information. Det ingår i det systematiska informationssäkerhetsarbetet och dataskyddsarbetet som ska finnas inom alla regioner och kommuner. Således är det här ett ständigt återkommande arbete för regionen liksom för alla andra organisationer som hanterar information. Processen för det systematiska informationssäkerhetsarbetet är ett stöd och vägledning då kompetensen för att genomföra de principer och arbetssätten ofta efterfrågas. Informationsinsatser kommer fortsatt att genomföras för det systematiska informationssäkerhetsarbetet.

8.2 NIS-direktivet och NIS- lagstiftningen

Den 6 juli 2016 antogs ”The directive on security of network and information systems, the NIS directive, det s k NIS direktivet, av Europaparlamentet. Direktivet

har implementerats i den svenska lagstiftningen genom Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Lagstiftningen omfattar leverantörer av samhällsviktiga och digitala tjänster. Regionen omfattas utifrån området hälso- och sjukvård inklusive tandvård.

Reglerna ställer bland annat krav gällande säkerhetsåtgärder, incidentrapportering och tillsyn. Regelverket ställer krav på att de verksamheter som omfattas ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Här handlar det om att identifiera de system som kan vara kritiska för att den samhällsviktiga tjänsten, hälso- och sjukvård ink. tandvård ska kunna bedrivas.

Under 2022 har en uppdatering av NIS-direktivet skett. NIS- 2 direktivet ställer högre krav gällande kontinuitet för det systematiska och riskbaserade arbetet.

Ett arbete har under 2022 startats upp i samarbete med Hälso- och sjukvården, Folktandvården och IT. En kartläggning över de it- stöd som är kritiska har genomförts. Prioritering av dessa är under arbete.

8.3 Framtidens vårdinformationsstöd

Framtidens vårdinformationsstöd är en helhetslösning som omfattar grundläggande stöd för vårddokumentation, vårdadministration och läkemedel, stöd för operationsplanering, anastesi/intensivvård, obstetrik, cytostatika samt drifttjänst, support och underhåll. Det nya vårdinformationssystemet ska införas i regionen under början av 2024.

Under 2022 startades en ny informationssäkerhetsgrupp där alla regioner som ska införa det nya vårdinformationsstöd ingår. Informationssäkerhetssamordnare ingår i gruppen. Ett omfattande arbete lades ner på acceptanstester under oktober månad. Acceptantesterna byggde på att verifiera dokumentation ur perspektivet information- och it- säkerhet. Gruppen kommer fortsatt arbeta aktivt under 2023 med informations- och it- säkerhetsfrågor. Ett arbete inom regionen har initierats för att på regional nivå under 2023 genomföra informationsklassning, riskanalyser, Konsekvensbedömning (DPIA) samt kontinuitetsplanering kopplat till det nya vårdinformationssystemet.

8.4 Upphandling och kravställning

Informationsklassning och riskanalys ska alltid föregås av en upphandling eller anskaffning då kraven för den informationsmängd som ska hanteras är specifik.
En del av de krav som framkommer utifrån en informationsklassning kan ses som generella krav och kan därför hanteras på ett enklare sätt.

Ett arbete har påbörjats gällande generell kravställning kopplat till informationssäkerhet vid upphandling och anskaffning inom regionen. Arbetet sker genom grupparbete där it- säkerhetsansvarig, informationssäkerhetssamordnare, upphandlingsjurist, informationssäkerhetshandläggare hälso-och sjukvården samt representanter från Regionservice medicinsk teknik deltar.